REMARKS

In the Official Action mailed on **March 8, 2004,** the Examiner reviewed claims 1-26. Claims 1-5, 7-11, 13-17, 19-24, and 26 were rejected under 35 U.S.C. §102(a) as being anticipated by Aziz (USPN 6,026,167, hereinafter "Aziz"). Claims 6, 12, 18, and 25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Aziz in further view of Tatebayashi et al.(USPN 6,151,394, hereinafter "Tatebayashi").

Amendments to the specifications

Applicant has amended the paragraphs starting on page 9, line 20 and page 11, line 3 to correct typographical errors. No new matter has been added.

Rejections under 35 U.S.C. §102(a) and 35 U.S.C. §103(a)

Independent claims 1, 7, 13, 19, 20, and 26 were rejected as being anticipated by Aziz. Applicant respectfully points out that Aziz teaches **utilizing a group interchange key** to encrypt a randomly generated transient key and encrypting a data packet using said transient key (see Aziz, col. 17 lines 4-40, col. 3 lines 7-9). Additionally, Aziz teaches periodically changing the group interchange key as a damage limitation feature in case of compromised interchange keys while performing Diffie-Hellman exchange (see Aziz, col. 11 line 60 to col. 12 line 16).

In contrast, the instant application discloses a key exchange system that uses **three** keys including (1) a negotiated secret key, (2) a group secret key, and (3) a pre-shared secret key. The negotiated secret key is obtained by performing a Diffie-Hellman exchange between the first and second parties. The group secret key is maintained by the group through a separate mechanism, and each user within the group has its own pre-shared secret key within a table of pre-shared secret keys. The present invention encrypts an identifier for the first party using

both the negotiated secret key and the group secret key to form an encrypted identifier (see page 8, lines 20-22 of the instant application). Note that using only a single key selected from a group of keys as Aziz teaches (see Aziz col. 3 lines 23-31) can result in **compromised keys** if an attacker intercepts communication between the first and second parties during the Diffie-Hellman exchange that is performed to obtain the negotiated secret key (see Aziz, col. 11 line 60 to col. 12 line 16). In contrast, using **both** the negotiated secret key and the group secret key for encryption is advantageous because it protects the identifier from an active attacker. An active attacker who can possibly obtain the negotiated secret key by intercepting communications between the first and second party during the Diffie-Hellman exchange is prevented from decrypting the identifier due to lack of the group secret key.

Additionally, the instant application discloses the decrypted identifier is used to look up a **third key**, a pre-shared secret key, within a table of pre-shared secret keys that are accessible only to the users within the group. This prevents access to the pre-shared key by any attackers, and thus prevents a given user from impersonating another user.

There is nothing within Aziz, or Tatebayashi, either separately or in concert, which would suggest using both a negotiated secret key and a group secret key for encryption and decryption of the identifier, and additionally performing a lookup in a table of keys for a third pre-shared secret key for encryption and decryption purposes. Using these three different types of keys obtained from different sources makes the present invention significantly more secure than the system described in Aziz.

Accordingly, Applicant has amended independent claims 1, 7, 13, 19, 20, and 26 to clarify that the system uses both the negotiated secret key and a group secret key to encrypt and decrypt an identifier, and that this identifier is subsequently used to retrieve a pre-shared secret key. These amendments find support on page 8, lines 20-26 and page 9, lines 16-19 of the instant application.

Dependant claims 2, 8, 14, and 21 have been cancelled without prejudice. Dependent claims 3, 9, 15, and 22 have been amended to correct antecedent basis.

Hence, Applicant respectfully submits that independent claims 1, 7, 13, 19, 20, and 26 as presently amended are in condition for allowance. Applicant also submits that claims 3-6, which depend upon claim 1, claims 9-12, which depend upon claim 7, claims 15-18, which depend upon claim 13, and claims 22-25 which depend on claim 20 are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 

Edward J. Grundler
Registration No. 47, 615

Date: April 9, 2004

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
508 Second Street, Suite 201
Davis, CA 95616-4692
Tel: (530) 759-1663
FAX: (530) 759-1665

INDEX NUMBER CHANGED

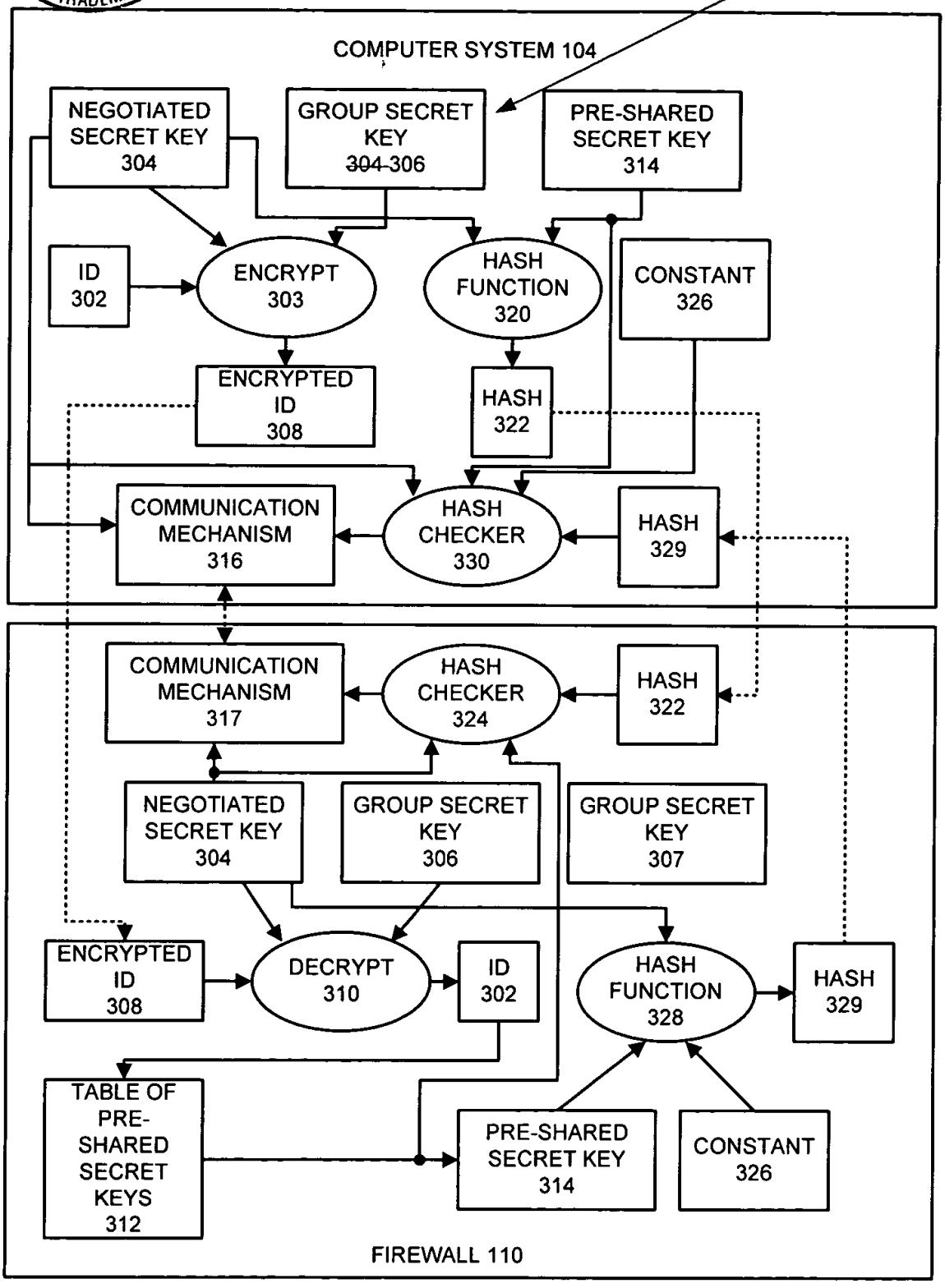

FIG. 3

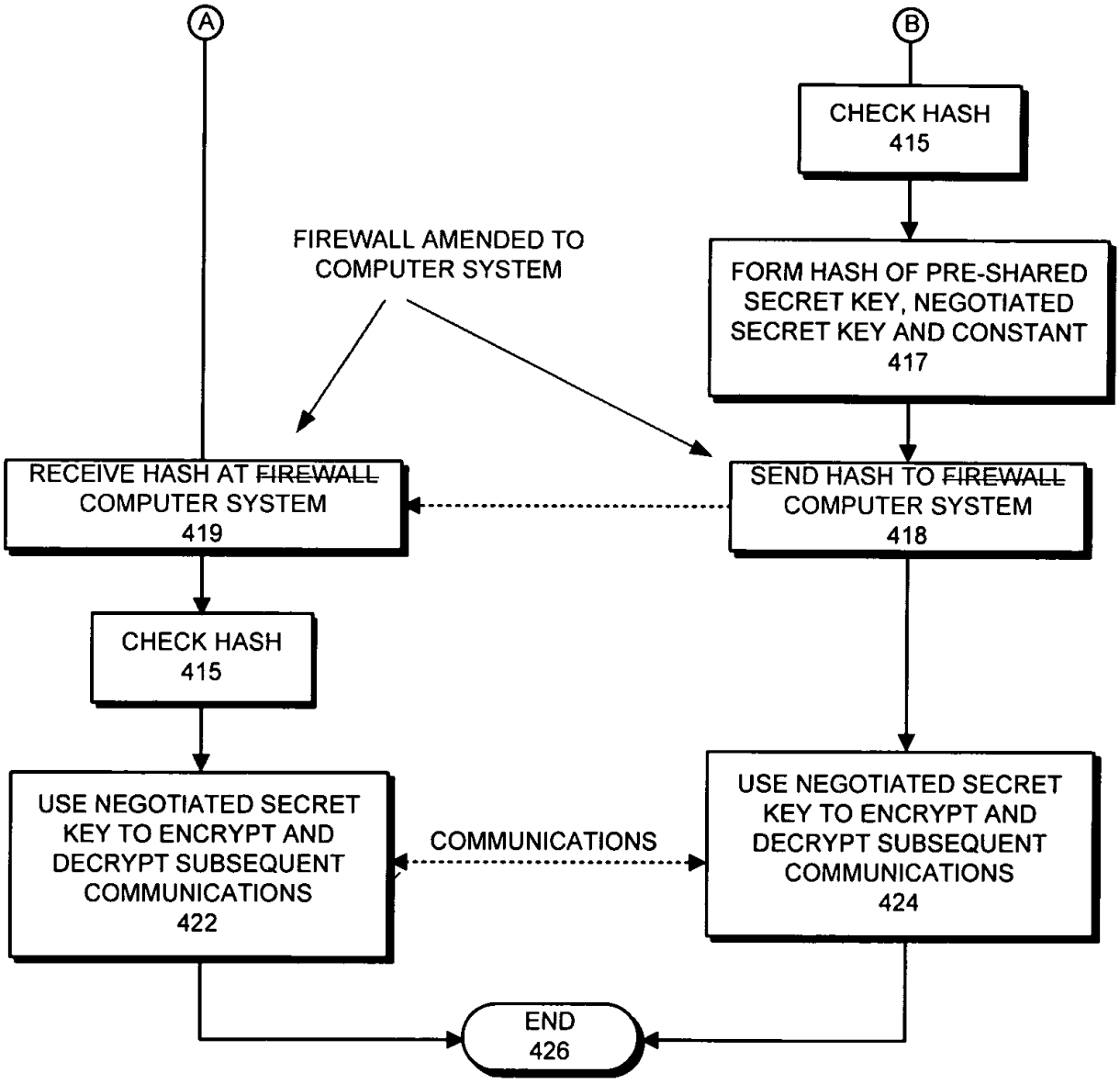

FIG. 4B